Commonwealth of Kentucky
Cabinet for Health and Family Services

Cabinet for Health and Family Services (CHFS) Information Technology (IT) Policy

010.103 Change Control

Version 2.2
March 8, 2018

Revision History

Date	Version	Description	Author
6/21/007	1.0	Effective Date	CHFS IT Policies Team Charter
3/8/2018	2.2	Revision Date	CHFS OATS Policy Charter Team
3/8/2018	2.2	Review Date	CHFS OATS Policy Charter Team

Sign-Off

Sign-off Level	Date	Name	Signature
IT Executive, Office of the Secretary (or designee)	3/8/2018	Jennifer Harp	Jennifer H. Harp
CHFS Chief Information Security Officer (or designee)	3/8/2018	DENNIS E. LEBER	

Table of Contents

Policy Definitions

- **Confidential Data:** Defined by COT standards, is data of which the Commonwealth has a legal obligation not to disclose. This data requires the highest levels of restrictions, because of the risk or impact that will result from disclosure, modifications, breach, or destruction of that data. Examples would include, but are not limited to, data not releasable under the Kentucky State law, Protected Health Information, Federal Tax Information, and Social Security and Credit Card Numbers.
- **Data Classification- NIST High Impact Level:** Severe or catastrophic effect on organizational operations, organizational assets, or individuals resulting in severe degradation to or a complete loss of an organization's ability to carry out its mission, severe financial loss, and/or catastrophic harm to individuals involving loss of life or serious life threatening injuries.
- **Data Classification- NIST Moderate Impact Level:** Serious adverse effect on organizational operations, organizational assets, or individuals including resulting in significant degradation to an organization's ability to carry out its mission, significant financial loss, and/or significant but non-life-threatening harm to individuals.
- **Data Classification- NIST Low Impact Level:** Limited adverse effect on organizational operations, organizational assets, or individuals resulting in minor degradation to an organization's ability to carry out its mission, minor financial loss, and/or minor harm to individuals.
- **Dedicated Environments:** A dedicated Development and Test Environments would have exclusive use of specific services provided on a server. A dedicated environment could have functionally related applications, databases and report services.
- **Sensitive Data:** Defined by COT standards, is data that is not legally protected, but should not be considered public information and only be disclosed under limited circumstances. Only authorized users should be granted access to sensitive data. Examples include, but are not limited to, information identifiable to an individual (i.e. dates of birth, driver's license numbers, employee ID numbers, license plate numbers, and compensation information) and Commonwealth proprietary information (i.e. intellectual property, financial data, and more.)
- **Shared Environments**: A shared environment is any environment where non-related application, database, report, or other services for different application platforms (Development, Test, Training, and Production) are housed on the same server. Multiple applications hosted on the same server are also considered shared environments.

010.103 Change Control

Category: 010.000 Logical Security

1 Policy Overview

1.1 Purpose

The Cabinet for Health and Family Services (CHFS) Office of Administrative and Technology Services (OATS) must establish an acceptable level of security controls to be implemented through a change control policy. This document establishes the agency's Change Control Policy which helps manage risks and provides guidelines for security best practices regarding change control.

1.2 Scope

The scope of this policy applies to all internal CHFS employees, consultants, temporary personnel, third party providers under contract with a CHFS agency, and other entities that interact with CHFS information related resources. This policy covers the applicable computer hardware, software, application, configuration, business data, and data communication systems. External vendors or other defined groups/organizations providing information security or technology services may work with the CHFS agency(s) to request exceptions to this policy.

1.3 Management Commitment

This policy has been approved by OATS Division Directors, CHFS Chief Technical Officials, and Office of the Secretary IT Executive. Senior Management supports the objective put into place by this policy. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of CHFS property (physical or intellectual) are suspected, CHFS may report such activities to the appropriate authorities.

1.4 Coordination among Organizational Entities

OATS coordinates with other organizations or agencies within the Cabinet with access to applications or systems. All organizational entities that interact with CHFS systems, within or contracted by OATS, are subject to follow requirements outlined within this policy. External vendors, or other defined groups/organizations, providing information security or technology services may work with the CHFS agency(s) when seeking exceptions to this policy.

1.5 Compliance

As the official guidance domain for this policy, CHFS agencies abide by the security and privacy requirements established in state laws and regulations as well as federal guidelines outlined in the National Institute of Standards and Technology (NIST). Applicable agencies additionally follow security and privacy frameworks outlined within the Centers for Medicare and Medicaid Services (CMS), the Internal Revenue Services (IRS), and the Social Security Administration (SSA).

2 Roles and Responsibilities

2.1 Chief Information Security Officer (CISO)

This positon is responsible for the assessment, planning, and implementation of all security standards, practices, and commitments required. This position is responsible to adhere to this policy.

2.2 Security/Privacy Lead

Individual(s) is designated by the division leadership to coordinate privacy and/or security issues and incidents with all appropriate personnel. This individual(s) is responsible for providing privacy and security guidance for protection of Personally Identifiable Information (PII), Electronic Personal Health Information (ePHI), Federal Tax Information (FTI) and other sensitive information to all CHFS staff and contractor personnel. This is role along with the CHFS OATS Information Security (IS) Team is responsible for the adherence of this policy.

2.3 Health Insurance Portability and Accountability Act (HIPAA) Privacy Officer

An attorney within CHFS Office of Legal Services (OLS) fills the Health Insurance Portability and Accountability Act (HIPAA) Privacy Officer position. This position is responsible for conducting HIPAA mandated risk analysis on information provided by the CISO or CHFS OATS Information Security (IS) Team. The HIPAA Privacy Officer will coordinate with the Information Security Agency Representative, the CISO, or CHFS OATS IS Team, and other CHFS agencies to ensure compliance with HIPAA notification requirements in the event of a breach. This position is responsible for reporting identified HIPAA breaches to Health and Human Services (HHS) Office of Civil Rights (OCR) and keeping records of risk analyses, breach reports, and notifications in accordance with HIPAA rules and regulations.

2.4 CHFS Staff and Contractor Employees

All CHFS staff, contract employees, and other applicable vendor/contract staff must adhere to this policy. All personnel must comply with referenced documents that pertain to the agency’s applications, application servers, appliances, operating systems, web servers, network components, and database (server or components) that reside on CHFS/OATS information system(s).

2.5 System Data Owner and System Data Administrators

It is the responsibility of these management/lead positons, to work with the application's development team to document components that are not included in the base server build and ensure backup are conducted in line with business needs. This individual(s) will be responsible to work with Enterprise, agency, and application technical and business staff to provide full recovery of all the application functionality and meet federal and state regulations for disaster recovery situations.

3 Policy Requirements

3.1 General Change Control

The Change Control Policy was implemented to establish unified control for changes to all servers. The Change Control Board (CCB) was established to ensure that the Change Control Policy is implemented and maintained as published. All data fixes shall be logged and recorded by the appropriate agency, and shall be auditable. CCB approval must be obtained for any data fix that requires a database restart or system reboot.

3.2 Description of Components

CHFS IT has implemented a change control process consisting of, but not limited to, an online change control portal, a weekly meeting with designated CCB, and an emergency approval contact list.

An online portal for the purpose of submitting, reviewing, and monitoring all change controlled processes has been established. The availability of this portal has been limited to technology personnel. The change control portal may be accessed via: https://webapp.chfsinet.ky.gov/ITMP/home.aspx.

The CCB carries the responsibility of managing all change control requests. This responsibility consists of the review, approval, denial and referral of such requests. The CCB shall consist of at least one representative of each affected branch within OATS. The CCB shall meet weekly at a designated and published time (this can be by conference call.) The CCB does not possess the responsibility to verify the technical feasibility of requested changes. This responsibility falls on the requestor or requestor's designee. Nor does the CCB act in place of management approval. All requests must be planned and cleared by all normal internal processes before a change control request is submitted.

The emergency approval designees hold the responsibility for approving all requests deemed an emergency. This shall consist of a primary and a secondary contact. There is an accurate assumption that such requests should receive a response within three (3) hours. If there is an occasion when no response is received for an emergency request within three hours, the request should be forwarded to the CCB Chairperson and/or upper level executive management.

3.3 Change Control Process: Production and Training Systems Environment

No change, including but not limited to; Hardware, Operating System, System Restarts and Application, shall be applied to a production system without the submission and prior approval of the standard Change Control Request process.

All CCB approved requests must be submitted to the Commonwealth Office of Technology's (COT) Change Advisory Board (CAB) for final approval and action.

3.4 Change Control Process: Development and Test Systems Environment

Dedicated Development and Test Environments have exclusive use of specific services provided on a server. All changes to non-production, except Development, (application modifications, database modifications, etc.) shall be entered into the ITMP change control portal for documentation purposes only. Lower environment change controls do not require CCB approval.

For Shared Development and Test Environments, no change concerning any modification of hardware, operating systems, installation of new applications, databases (i.e. SQL, Oracle), or system restarts shall be applied to a non-production, shared system without the submission and prior approval of a change control request to the CCB. All other changes (application modifications, database modifications, etc.) shall be entered into the change control portal for documentation purposes only.

3.5 Request Submission

All testing, planning, notification and management approval must be completed prior to submitting a change control request. Upon submission, all requests must be completed as fully as possible. Failure to complete a required task, provide proper, adequate or required information may result in the denial or delay of the change request.

Change requests must be submitted in a timely manner. All non-emergency requests shall be reviewed weekly during the regularly scheduled change control meeting. All requests received after 10:00 am, the morning of the scheduled meeting, shall be reviewed during the following week's CCB meeting.

Careful evaluation must be applied to the following areas when submitting a change control request:

Risk Factor Level	Risk Factor Description
Minimum	Little to no impact of current services
Medium	Clear and noticeable impact of services
Severe	Significant impact on the services and the business. Considerable manpower and/or resources needed.

Impact Level	Impact Description
Low	Change leads to minor improvement
Medium	Change will solve irritating errors or missing functionality
High	Change needed as soon as possible (Potentially damaging)
Emergency	Change necessary now (Otherwise severe business impact) *May not be applicable to scenarios that could have/should have been planned

Upon submittal of a change control request, the request shall be assigned to the next available change control meeting. During this time the CCB will review the request, verify scheduling and access project impact. Once the CCB has made their decision, the requestor shall be notified.

Upon CCB approval of a change control request, the requestor may proceed with the change. If the scheduling and/or scope of the change varies from the approved request, then the change control must be postponed and resubmitted for approval.

Upon denial of a change control request, all intended operations must be stopped. The requestor may view the change control request for comment from the CCB and resubmit accordingly.

If there is a change of status for any request, including completion of tasks, it is the requestor’s responsibility to review and update the request.

Prior to CCB approval, the requestor would submit their request to the Commonwealth Service Desk (CommonwealthServiceDesk@ky.gov) to open a ticket. If a vendor is completing the release, the ticket will be used for either assistance or information. If available, all requests must include documentation with release instructions.

4 Policy Maintenance Responsibility

The OATS IS Team is responsible for the maintenance of this policy.

5 Policy Exceptions

Any exceptions to this policy must follow the guidance established in CHFS OATS Policy: 070.203- Security Exceptions and Exemptions to CHFS OATS Policies and Security Control Policy.

6 Policy Review Cycle

This policy is reviewed at least once annually, and revised on an as needed basis.

7 Policy References

- Centers for Medicare and Medicaid Services (CMS) MARS-E 2.0
- CHFS OATS Policy: 065.014 CHFS SDLC and New Application Development Policy
- CHFS OATS Policy: 070.203- Security Exceptions and Exemptions to CHFS OATS Policies and Security Control Policy
- Enterprise IT Procedure: COT-009- Change Management Procedure
- Enterprise IT Procedure: COT-067- Enterprise Security Standard Process and Procedure Manual (ESPPM) Process
- Internal Revenue Services (IRS) Publication 1075
- National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations
- Social Security Administration (SSA) Security Information